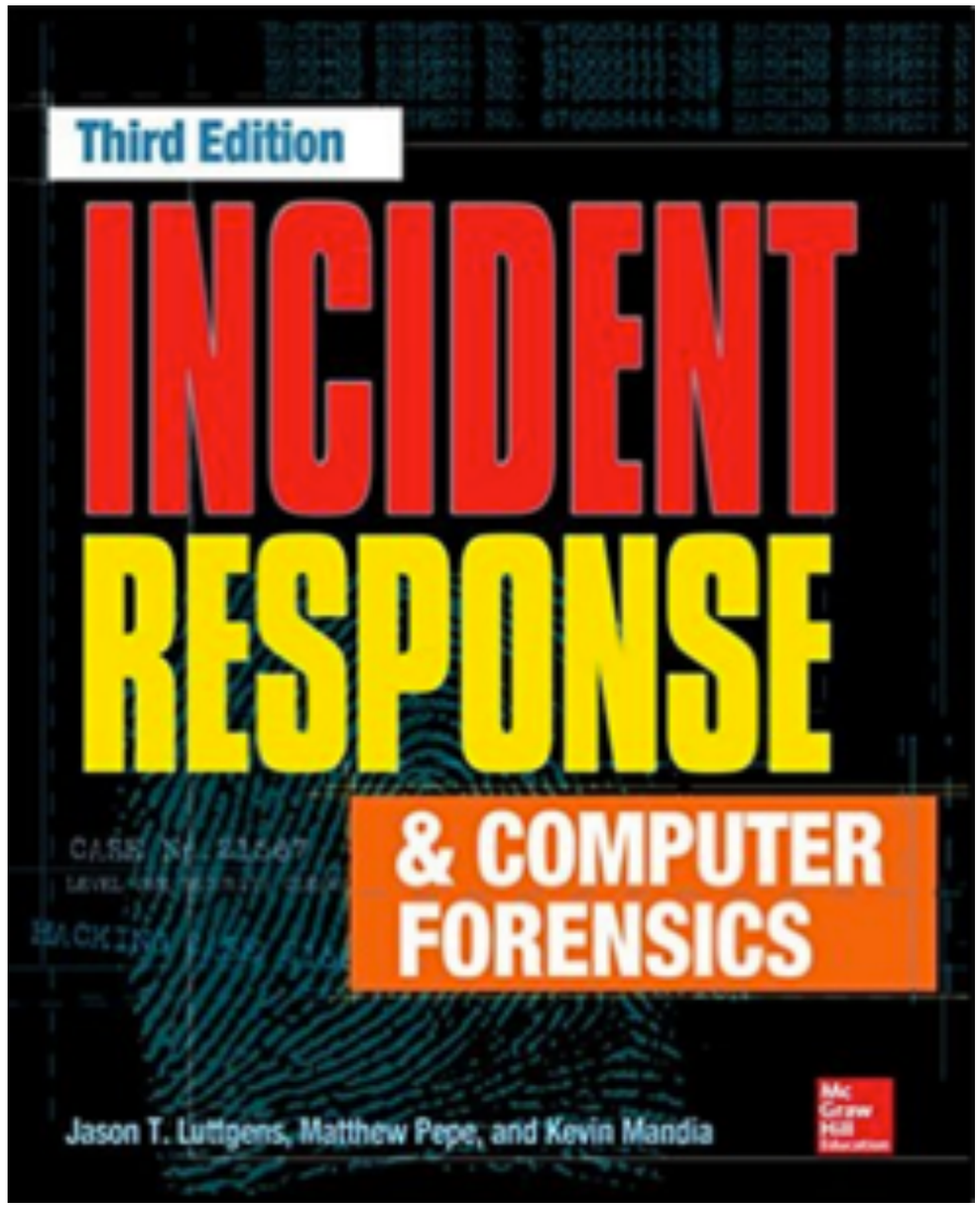
CNIT 152: Incident Response



6. Discovering the Scope of the Incident

Updated 9-15-22

Establishing the Scope

- **Examining initial data**
- **Gathering and reviewing preliminary evidence**
- **Determining a course of action**

Examining Initial Data

- **Look at original alert**
- **You may notice more than the person who reported it did**
- **Ask about other detection systems and review what they recorded**
- **Network administrators may not think like investigators**
- **Gather context for the detection event**

Preliminary Evidence

- **Determine what sources of preliminary evidence may help**
- **Decide which sources you will actually use**
- **Collect and review the evidence**
- **Identify sources that are easy to analyze, and that quickly provide initial answers**

Example: Malware

- **Artifacts the malware directly creates on the system, such as files or registry keys**
- **Operating system artifacts, such as Windows prefetch, that are indirect artifacts**
- **Application artifacts, such as Internet browser history or software metering tools**
- **Network artifacts, such as firewall logs that might record network connections**

Independent Sources

- **Firewall logs don't depend on registry keys, etc.**
- **Multiple independent evidence sources lead to more reliable conclusions**
- **It's difficult for an attacker to remove or modify evidence from all sources**
- **Less likely that a routine process would overwrite or discard all evidence**
- **Cross-check information, like date and time**

Review

- **Attacker may be causing more damage**
- **Test a detection method on one system, or a small date range of log entries**
- **Make sure your detection method is fast and effective**

Determining a Course of Action

- **Will the action help answer an investigative question?**
- **Will the action answer my questions quickly?**
- **Am I following the evidence?**
- **Am I putting too much effort into a single theory?**

Determining a Course of Action

- **Am I using multiple independent sources of evidence?**
- **Do I understand the level of effort?**
- **Am I staying objective?**
- **Am I tracking the earliest and most recent evidence of compromise?**
- **Have I uncovered something that requires immediate remediation?**

Scenario1:
Data Loss

Data Loss Scenario

- **Large online retailer**
- **You work in IT security department**
- **Customers are complaining about spam after becoming a new customer**

Finding Something Concrete

- **Anecdotal customer complaints are inconclusive**
- **Options**
  - **Work with customers and review their email**
    - **Reliability and privacy problems**
  - **Create fake customer accounts with unique email addresses**

Fake Accounts

- **Use 64-character random usernames**
- **Unlikely that spammers would guess the usernames**
- **Monitor those accounts**

Preliminary Evidence

- **Assuming customer data is being lost somehow**
  - **Find where customer data is and how it is managed**
- **One internal database on production server**
- **One external database at a third-party marketing firm**

Interview Results

- **The customer database system is a mainstream commercial product, with advanced query monitoring and reporting capabilities.**
- **The database is approximately 500GB (gigabytes) in size.**
- **The database network traffic is approximately 3TB (terabytes) per day.**
- **Customer records are updated directly via the company website or manually via phone call into the customer service department.**

Interview Results

- **No other method of updating customer records exists.**
- **Backups are kept both on-site and off-site at another of your company's facilities.**
- **The marketing firm receives data at the end of the month following any updates.**

Progress

- **It's unlikely the marketing firm is a source of the data loss, because, according to the customers' complaints, spam was received sooner than the firm received the data.**
- **Theft of customer records via customers calling in via phone seems unlikely; therefore, any investigative focus on the data input side would concentrate on the website.**
- **The volume of network traffic to the database is high, so performing a network packet capture may be difficult, if required. Because the database supports advanced query monitoring, this may be a better method to monitor database access.**

Theories & Simple Tests

- **Insider**
  - **No easy way to test**
- **Modified code on website to capture email addresses**
  - **Enter some fake accounts directly into database, bypassing the web form**
- **Someone copying backup tapes**
  - **Add some fake accounts to the backups**

Three Sets of Fake Accounts

1. **Made through the web form**
2. **Entered directly into the database, bypassing the web form**
3. **Added only to the backups**

Two Weeks Later

- **Spam comes to the first set of fake accounts**
- **And to the accounts manually entered into the database**
  - **Suggests the website is not part of the problem**
- **No spam to the accounts on the backup tape**
  - **Backups aren't the source of data loss**

New Theories

- **Direct access to the database**
  - **Malware on the database server**
  - **Accessing it over the network**

Monitoring Queries

- **Network-level packet captures**
  - **Expensive, powerful system required**
  - **If queries are encrypted, or malware is obfuscating them, it may be hard to decode the traffic**
- **Database-level query monitoring and logging**
  - **Most efficient and reliable technique**

Next Steps

- **Create a few more fake accounts**
- **Talk to database and application administrators**
  - **To find out where data is stored**
- **Scan through logs to see what is "normal"**
- **No queries or stored procedures perform a bulk export of email addresses on a daily basis**

Two Weeks Later

- **New accounts get spam**
- **Retrieve query logs from time accounts created to spam time**
  - **For the field "custemail"**
- **A single query is found**
  - **SELECT custemail FROM custprofile WHERE signupdate >= "2014-02-16"**

Query Details

- **Feb 17, 2014 at 11:42 am GMT**
- **Originated from IP in graphics arts dept.**
- **Query used an database administrator's username from the IT dept.**
- **Interview reveals that graphics arts dept. has no direct interaction with customers, only outside vendors**

Leads

- **There is evidence to support complaints of people receiving spam shortly after becoming a new customer.**
- **Preliminary data suggests a two-week cycle of data theft that only includes a customer's e-mail address. The data is being extracted directly from the production database.**
- **Database queries are made over the network, originating from a desktop computer in the graphic arts department. The department does not use customer e-mail addresses are part of their normal business processes. Additionally, the query uses a database user ID that belongs to a database administrator in the IT department.**

Action: Graphics Arts Desktop

- **Collect a live response.**
- **Create forensic images of memory and the hard drive.**
- **Interview the user and determine the following:**
  - **How long the system has been assigned to them**
  - **If they've noticed anyone using it who shouldn't be**
  - **If the system has been "acting strange"**
  - **If the system is left on 24 hours a day, seven days a week**

Action: Database Server

- **Collect a live response.**
- **Preserve all database logs that record user access.**
- **Preserve all query logs.**
- **Preserve all application and system logs.**

Results from Workstation

- **Examine images, focusing on actions at the time of the query**
- **Malware found on workstation**
  - **Persistent, provides remote shell, remote graphical interface, ability to launch and terminate processes**
  - **Connects to a foreign IP**
  - **Has been installed for two years**
  - **Cannot determine how system was originally compromised**

Final Steps of Investigation

- **Use a host-based inspection tool to examine each computer in your enterprise for indicators of compromise—file names, registry keys, and other unique characteristics of the malware.**
- **Query firewall logs for indications that other computers may be infected—traffic to the IP address the malware connects to.**

Scoping Gone Wrong

- **After complaints from customers**
  - **Search every computer in the company for unique strings in the customer data,**
  - **And files large enough to include all the customer records**

Problems

- **No evidence that the stolen data is stored on company servers**
- **No evidence that the data is all being stolen at once in a large file**
  - **And even so, it would probably be compressed**
- **Large amount of effort; low chance of success**

Another Unwise Path

- **Focus on insiders**
  - **Who had access and knowledge to steal the customer data**
    - **Compile profiles of numerous employees**
    - **Review personnel files**
    - **Background checks, surveillance software capturing keystrokes and screen images**
    - **Video surveillance installed**

Problems

- **Leads to a "witch hunt"**
- **Invades privacy of employees**
- **Large effort, small chance of success**

Another Unwise Path

- **Because the data resides on the database server**
- **Image and analyze RAM from the database server to hunt for malware**
  - **Because the hard drives are massive and too large to investigate easily**

Problems

- **Once again, they have jumped to a conclusion**
- **And ignored other possibilities**
- **Large effort, low chance of success**

Scenario 2: Automated Clearing House Fraud

Funds Transfer

- **Bank called the CEO--they blocked an ACH transfer of $183,642.73**
  - **To an account that was never used before**
  - **Flagged by their fraud prevention system**
- **Transfer from CFO's account, but he says he never authorized it**

Facts from the Bank

- **The transfer request was initiated online using your CFO's online banking account.**
- **The requested transfer amount was US$183,642.73.**
- **The transfer request was initiated one day ago, at 4:37 P.M. GMT-5 (EST).**
- **The source IP address was your company's public Internet IP address (your firewall).**

Preliminary Evidence

- **Firewall**
  - **Two weeks of logs**
    - **Examine this first**
- **Should you examine CFO's laptop computer?**
  - **Live response, RAM, hard drive**
  - **But maybe other computers are involved**

Firewall Logs

- **Look near the time the unauthorized transfer occurred (4:37 pm)**
  - **See who logged in prior to that**
- **Two computers logged in via HTTPS, making a number of connections between 4:10 pm and 4:48 pm**
- **From two IPs -- one is CFO's, other not immediately recognized**

Two Immediate Tasks

- **Gather complete forensic evidence from CFO's computer**
  - **Live response, RAM, and hard disk**
  - **Because evidence is being lost as time passes**
- **Track down the other IP address and decide what action is appropriate**

DHCP Logs

- **Search for the time in question**
- **Get MAC address from DHCP logs**
- **It's the MAC of the CFO's laptop (wireless card)**
- **So there's only one computer involved**

Interview the CFO

- **The CFO was at work yesterday, but left for the day at 4:30 P.M.**
- **The CFO had a meeting just prior to leaving for the day. The meeting was held in the conference room, and during that time, the CFO says he used the company wireless network. The meeting was to compare your current bank's service offerings against a competitor. During that meeting, the CFO did access the bank's website, but did not use online banking.**
- **The CFO restates that he did not initiate the unauthorized transfer, and that he does not know anything about the destination account number associated with the transfer.**

Recap

- **A review of the firewall logs shows connections from your CFO's computer to the bank during the time frame in question. There were no connections from other computers.**
- **The CFO says he did not request the transfer, and, additionally, he was not in the office at the time of the transfer request. Your company does not provide remote access to computers left at the office.**
- **You have firewall logs for the past two weeks.**
- **You have live response data, memory, and hard drive images of the CFO's computer.**

Theories

- **Perhaps someone entered the CFO's office and used his computer—you could check the Windows event logs for logon events. You could also check security cameras to see if anyone entered the CFO's office.**
- **Maybe there is undetected malware on the CFO's computer, providing a remote attacker with access to the system—you could review the forensic data you collected for suspicious startup programs or artifacts created around the time in question.**

Open Office Space

- **CFO's office is in clear view of other workers**
- **It's unlikely that someone could go into it unobserved**

CFO's Computer

- **Recently installed persistent executable**
- **Send it to a third-party analysis site**
- **It's a variant of the Zeus banking malware**

Final Steps of Investigation

- **Conduct a thorough forensic examination of the CFO's computer. You still need to determine how and when the system was infected.**
- **Use a host-based inspection tool to examine each computer at your company for indicators of compromise—file names, registry keys, and other unique characteristics of the malware.**
- **Query firewall logs for indications that other computers may be infected—traffic to the IP address the malware communicates with.**

Scoping Gone Wrong

- **There are no recent antivirus or IDS alerts**
- **So you believe the security issue must be at the bank**
- **Tell the bank to find the attacker and put them in jail**

Problems

- **No attempt to validate the bank's original data**
- **Company assumes that existing network security measures would detect a problem, if there was one**
- **Assumption that a third-party can help you**
- **While you wait, data on company systems is lost**

Another Unwise Path

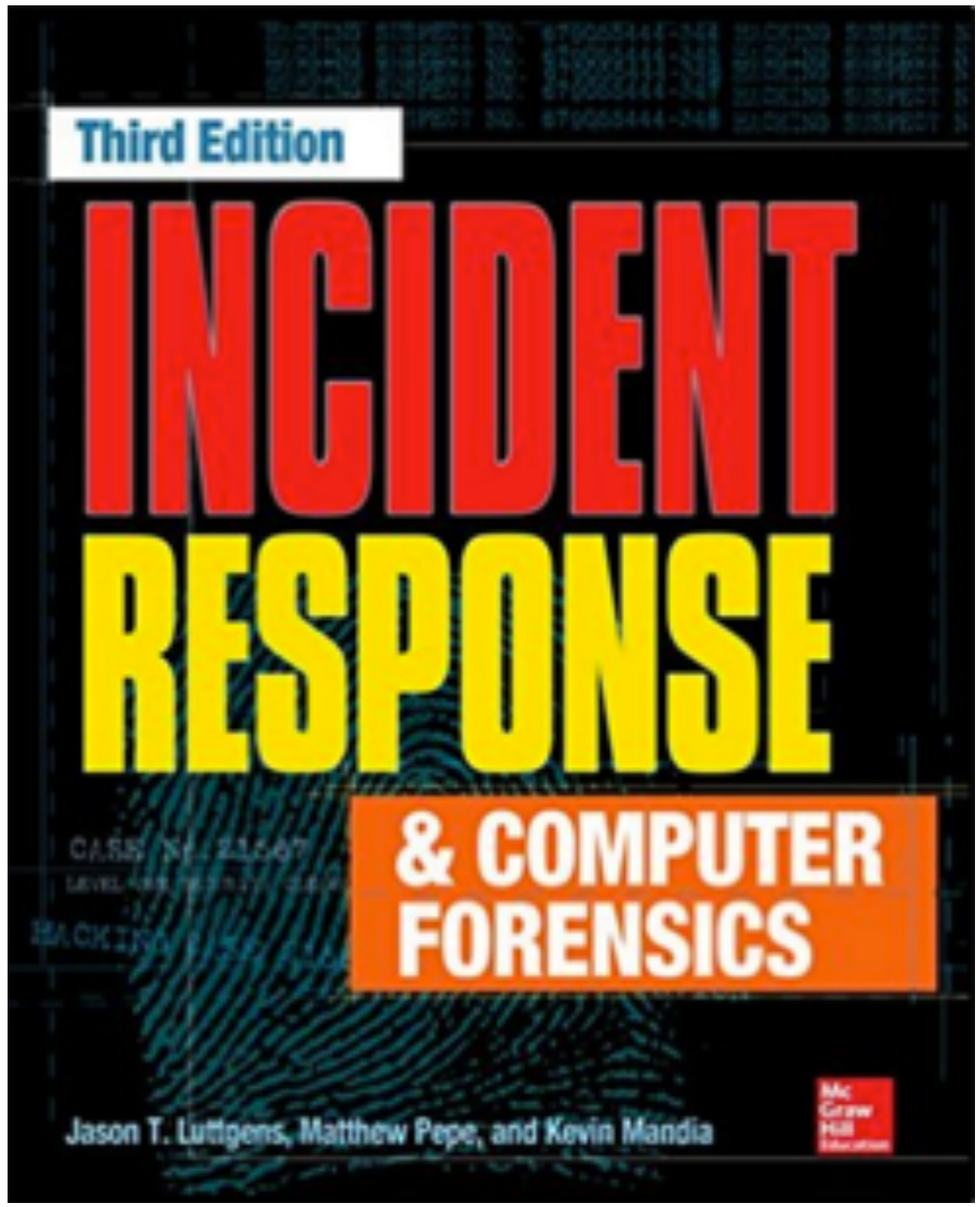
- **CEO believes that security measures are in place to prevent malware, so the CFO must have initiated the transfer**
- **The CEO wants you to investigate the CFO and avoid tipping him (or her) off**

Problem

- **No security measures are perfect, not even two-factor authentication**
- **Also, that sort of investigation is outside your expertise, and should be referred to an outside contractor**

Ch 6

CNIT 152: Incident Response



7. Live Data Collection

Purpose of Live Collection

- **Preserve volatile evidence that will further the investigation**
- **Also collect log files and file listings**
- **Get answers quickly**
- **Minimize changes to the system**
- **Avoid disrupting business, causing crashes, or destroying evidence**

When to Perform Live Response

1. **Is there reason to believe volatile data contains information critical to the investigation that is not present elsewhere?**
2. **Can the live response be run in an ideal manner, minimizing changes to the target system?**
3. **Is the number of affected systems large, making it infeasible to perform forensic duplications on all of them?**
4. **Is there risk that forensic duplications will take an excessive amount of time, or potentially fail?**
5. **Are there legal or other considerations that make it wise to preserve as much data as possible?**

Risks of Live Response

- **Have you tested the live response process on a similar system?**
- **Is the system particularly sensitive to performance issues?**
- **If the system crashes, what would the impact be?**
- **Have you communicated with all stakeholders and received their approval? In some cases, written approvals may be prudent.**

Altering the Evidence

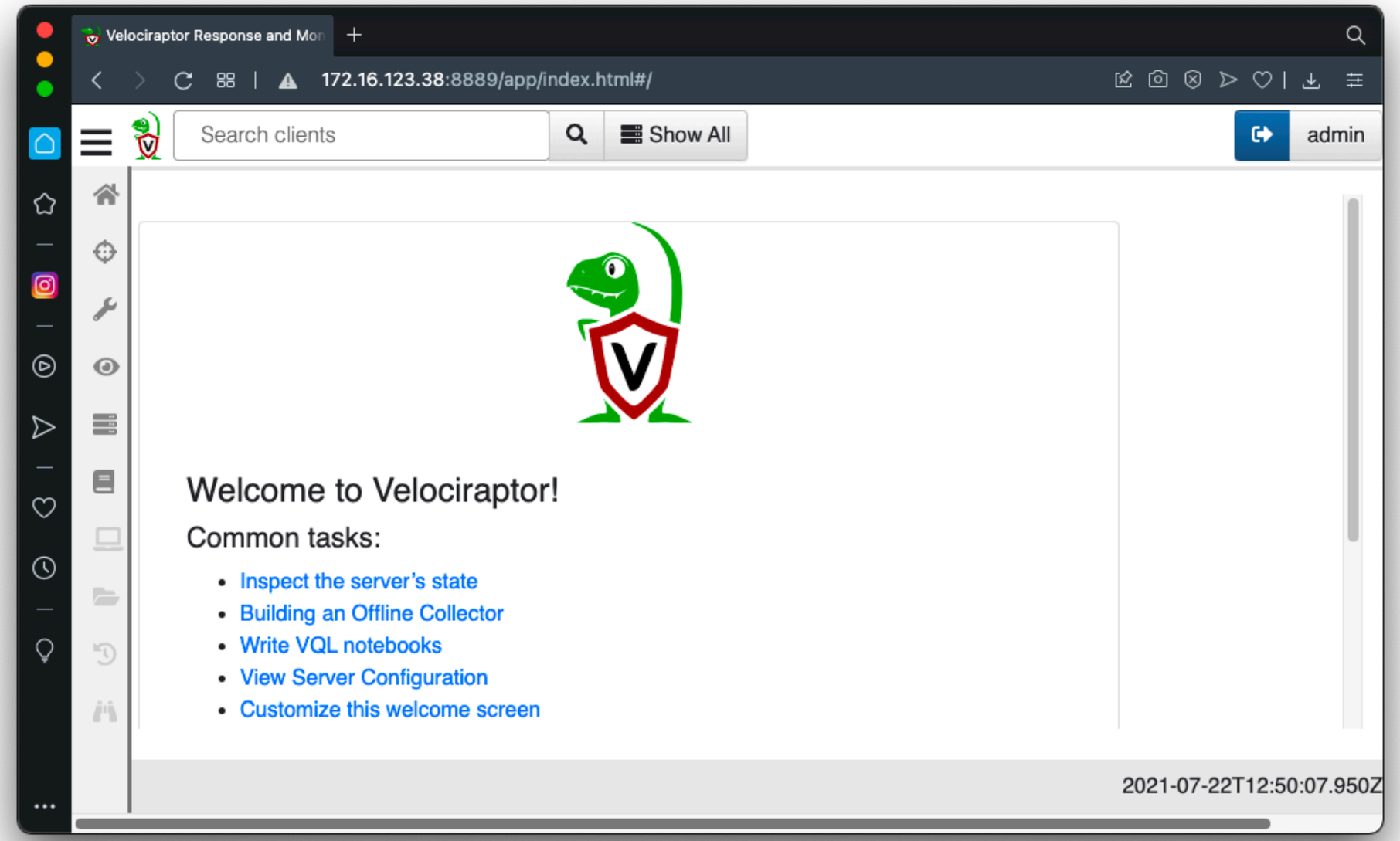
- **All live response changes the system**
  - **Purists don't like it**
    - **But the alternative is to lose all volatile data and get only a disk image**
- **You can minimize changes, but not eliminate them**

Selecting a Live Response Tool

- **Homegrown Microsoft DOS batch script (or bash)**
- **Perl-based script**
- **There are specialized live-response products, free and commercial**

Velociraptor

- Our main live response tool



Factors to Consider

- **Is the tool generally accepted in the forensic community?**
- **Does the solution address the common operating systems in your environment?**
  - **Tools that use OS commands should contain known good copies of those commands, not trust the local commands on the suspect system**

Factors to Consider

- **Does the solution collect data that is important to have, in your environment?**
- **How long does a collection take?**
  - **Recommended: less than an hour per system**
- **Is the system configurable?**
- **Is the output easily reviewed and understood?**

What to Collect

- **Current running state of the system**
  - **Network connections**
  - **Running Processes**
- **What happened in the past**
  - **File listings, system logs**
  - **Usually a higher priority**

The Deep End

- **Some organizations always collect entire RAM contents, or hard disk images**
  - **Don't collect data that you can't effectively use or understand**
- **Collect data you can really use to quickly determine the impact of the incident**

Data to Collect

- **The system time and date, including the time zone**
- **Operating system version information**
- **General system information, such as memory capacity, hard drives, and mounted file systems**
- **List of services and programs configured to automatically start on boot-up, such as web servers, databases, multimedia applications, and e-mail programs**
- **List of tasks scheduled to automatically run at given times or intervals**
- **List of local user accounts and group membership**

Data to Collect

- **Network interface details, including IP and MAC addresses**
- **Routing table, ARP table, and DNS cache**
- **Network connections, including associated processes**

Data to Collect

- **Currently loaded drivers or modules**
- **Files and other open handles**
- **Running processes, including details such as parent process ID (PID) and runtime**
- **System configuration data**
- **User login history, including user name, source, and duration**
- **Standard system log data**
- **List of installed software**
- **Appropriate application log data—web browser history, antivirus logs, and so on**
- **Full file system listing, including the appropriate timestamps for the file system**

Complete RAM Capture

- **Requires specialized tools to collect and interpret**
- **Not part of Live Response**
- **Sometimes needed on carefully chosen systems**

Collection Best Practices

- **Practice on a test system first**
- **Learn how fast the process is, and how large the output is**
- **Practice handling problems**
  - **Broken USB port or NIC**
  - **Locked screen**

Caution: Malware

- **The system you are examining may be infected with malware**
- **Any media you connect may become infected**
- **Any credentials you use may be compromised**

Recommended Procedure

- **Document exactly what you do and when you do it. You'll need to note the difference between the actual time and system time. Don't forget to include time zone in your notes.**
- **Treat the suspect computer as "hot"—do not interact with it unless you have a plan. Get on and off the system as quickly as possible.**
- **Use tools that minimize the impact on the target system. Avoid GUI-based collection tools; instead, use tools that have a minimal memory profile and that do not make unnecessary or excessive changes to the target system.**
- **Use tools that keep a log and compute cryptographic checksums of their output as the output is created (not after the fact).**

Comparison of Acquisition Software for Digital Forensics Purposes

Authors:

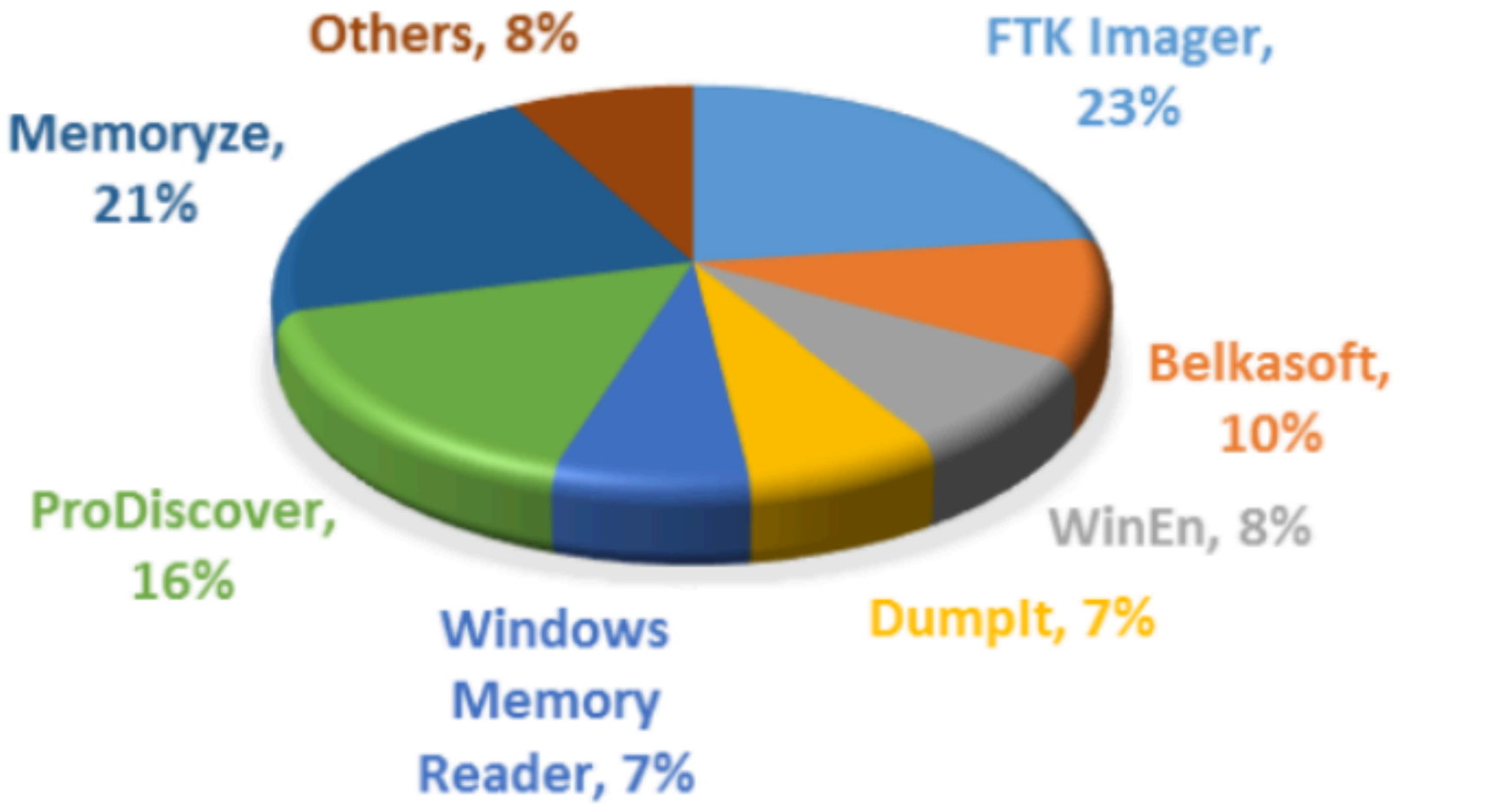
Muhammad Nur Faiz
Politeknik Negeri Cilacap

Wahyu Adi Prabowo
Institut Teknologi Telkom Purwokerto

- From 2018
- Link Ch 7f

- https://www.researchgate.net/publication/328859673_Comparison_of_Acquisition_Software_for_Digital_Forensics_Purposes

Popular Tools



41 Respondents in the USA

RAM Usage

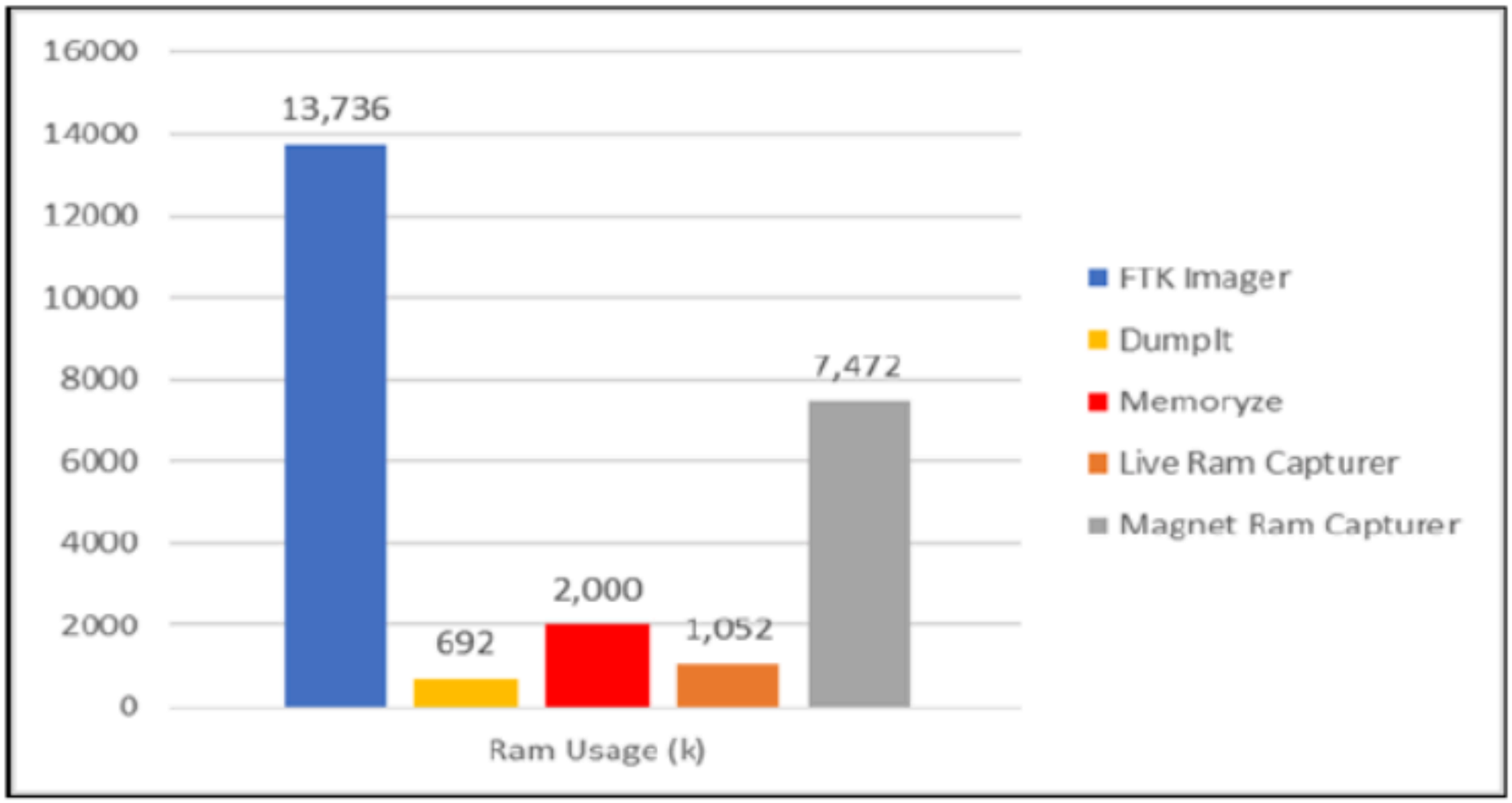


Figure 8. RAM Usage Acquisition Tools

DLLs and Registry Keys

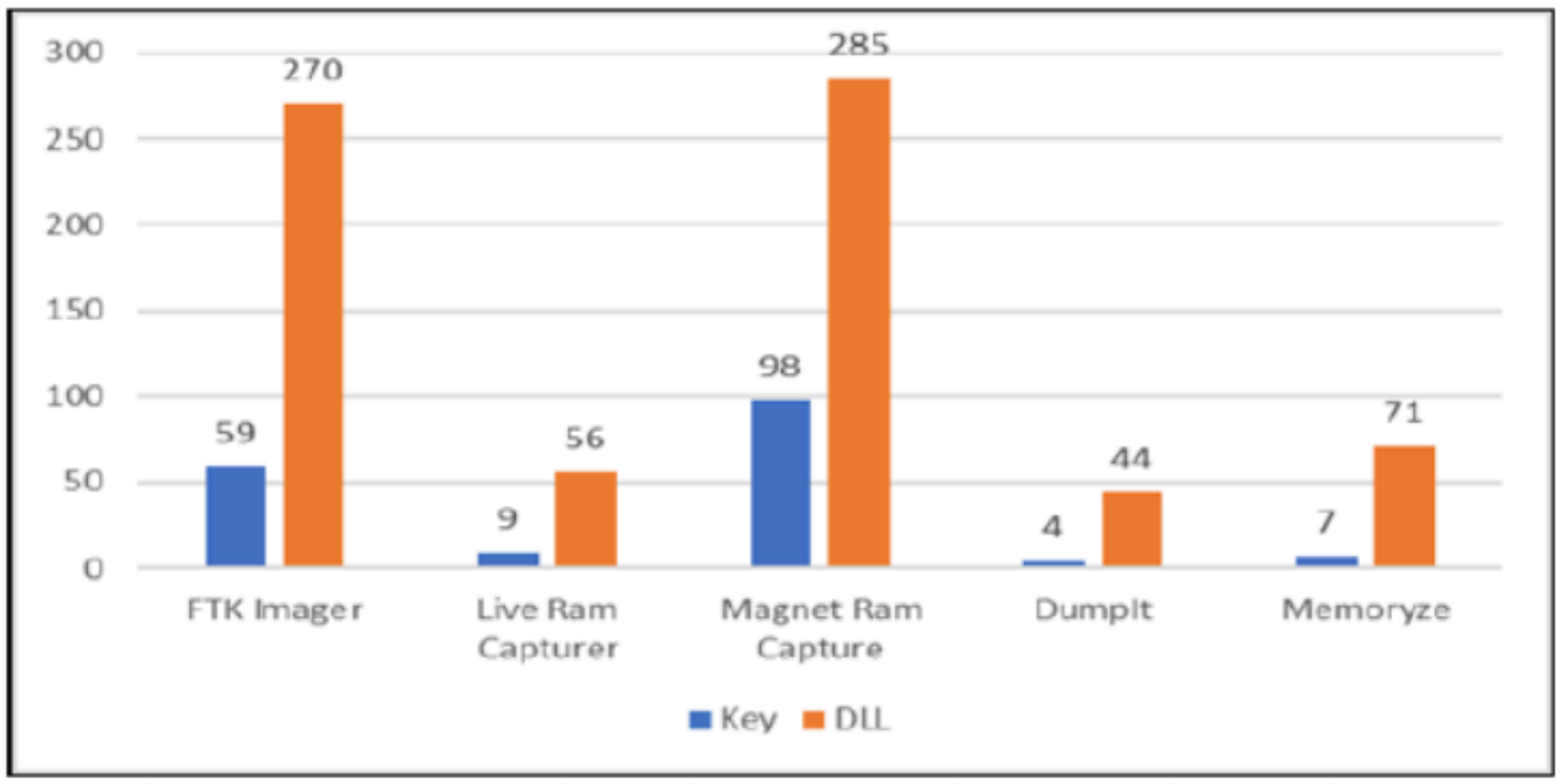


Figure 10. DLL and Registry Key of Acquisition Software

Results

Table 1. Comparison Acquisition Software

Tools	Memory Usage (Mb)	Processing Time (second)	Registry Key	DLL
FTK Imager	117	198.65	59	270
Belka RAM Capturer	18	186.22	9	56
Magnet RAM Capture	76	220.24	98	285
DumpIt	10	185.6	4	44
Memoryze	13	184.54	7	71

Recommended Procedure

- **Fully automate the collection process, perhaps eliminating the requirement for a human to interact with the suspect computer.**
- **Do your best to collect data in order of volatility.**
- **Treat the data you collect as evidence—be sure to follow your data preservation procedures, including the creation of an evidence tag and chain of custody. Don't forget to compute an MD5 checksum of the evidence.**
- **Consider files on media you connect to the suspect computer as lost to the attacker. For example, do not keep indicators, documents, reports, notes, or anything else on the media from which the live response will be run.**

Recommended Procedure

- **Consider any credentials you use as compromised. It's a good idea to use an account other than your primary account, and change the password frequently or use a two-factor or one-time password solution.**
- **Do not take actions that will cause unnecessary modifications to the suspect computer unless there is no other option, such as copying the live response kit to the system or storing the output there. Doing so may destroy valuable evidence. Use removable media, a network share, or other remote media options.**
- **Do not use the suspect computer to perform analysis. This causes unnecessary changes to the system, potentially destroying evidence and making it harder to discern attacker activity from responder activity. You also do not know what state the system is in—it could be providing incorrect results.**

Horror Stories: IR Procedures

- **Copy live response toolkit to affected systems, save collected data back to that same system including full RAM dump, several gigabytes in size**
- **Remotely log in with domain administrator account, run netstat & Task Manager**
- **Pull out the plug, image the hard drive**

Good Methods of Live Response

- **Network share on a dedicated file server**
  - **Not part of any domain**
    - **Used throwaway credentials not used for any other purpose**
- **Two folders**
  - **Read-only containing the live response toolkit**
  - **Writeable for output from live response toolkit**

Live Response Process

1. **Browse to the share (or map a drive letter) from the suspect system.**
2. **Run the live response program directly from the share and specify the output folder on the share as the location to write data. Ideally, a subfolder would be created using a unique identifier such as an evidence tag number.**
3. **Once the collection is complete, the responder returns to their desk and moves the live response data from the temporary share location to a separate server that permanently houses live response data and has appropriate access controls.**

Live Response Tips

- **Air-gap for evidence server**
- **Logging and auditing access to evidence server**
- **Automate process for consistency**
- **Live Response software must run as Local Administrator/root**

Media

- **Some computers cannot connect external media**
  - **Hardware failure, configuration, etc.**
- **Common options for running toolkit**
  - **CD-ROM, DVD, network share**
  - **Encrypted network streaming tool like cryptcat or stunnel to send output to another system**

Unexpected OS

- **Cannot run your normal live response toolkit**
- **If you can't update or modify your toolkit to run**
- **Perform manual live response**

Unexpected OS

- **Create a checklist of the automated steps in the toolkit for a similar OS**
- **Research command-line options**
- **Test them on a known clean system, if possible**
- **Manually perform steps to collect evidence**

Automation

- **Decreases human error**
- **Makes processes more consistent and faster**
- **Helps to prevent bad guys from gathering intelligence about how you respond to incidents**
- **Anything you do on the evidence system may be sent to the bad guys**

Ch 7a

Live Data Collection on Microsoft Windows Systems

Three Main Options

- **Use a prebuilt kit**
  - **Like Mandiant Redline or Velociraptor**
- **Create your own**
- **Use a hybrid of the two**

Mandiant Redline

- **Install the Redline MSI package on a trusted workstation**
- **Create the Redline collector on the trusted system**
- **The only step you take on a suspect system is to run the stand-alone Redline collector batch script**
- **Automatically saves data to the same location you ran the script from**

Do It Yourself

- **Make your own live response toolkit**
  - **Decide what OS to support**
    - **Windows has many versions, and big differences between 32-bit and 64-bit**
  - **Find tools that collect the information you want**

Windows Built-in Tools

- **Copy these files from a clean Windows system**
- **Also copy cmd.exe**
- **"Trusted binaries"**
- **Don't trust files on the evidence machine**

Data Collected	Command(s)
System date and time	date and time
Time zone Installed software General system information OS version Uptime File system information	systeminfo
User accounts	net user
Groups	net group
Network interfaces	ipconfg/all
Routing table	route print
ARP table	arp -a
DNS cache	ipconfig/displaydns
Network connections	netstat -abn

Free Tools

- **Use command-line versions, not GUI versions**
  - **Easier to script**
  - **Less impact**
- **Rename every tool so you can identify it as something you added to the system**
- **Prepend "t_"**

Data Collected	Tool Name
Network connections	DiamondCS openports (www.softpedia.com)
List of services and tasks	Microsoft autoruns
Loaded drivers	NirSoft DriverView
Open files and handles	NirSoft OpenedFilesView
Running processes	Microsoft pslist
Registry (config data)	Microsoft logparser
Event logs (login history)	Microsoft logparser
File system listing	Microsoft logparser
LR output checksum computation	PC-Tools.net md5sums or hashutils (code.kliu.org/misc/hashutils)

Other Data Items

- **Prefetch information**
- **System restore point information**
- **Browser history, and more**
- **Balance your needs with the impact the collection has on the system**

Scripting Language

- **Choose one**
  - **MS-DOS Batch (lowest impact)**
  - **PowerShell**
  - **VBScript**
  - **Perl**
  - **Python**

Scripting Tips

- **Add logging and compute a checksum of collected data**
- **Be careful with file and directory names**
  - **They may be long or include spaces**
- **Test your script extensively**
  - **Built a test environment that resembles your production systems**
  - **Watch for errors and unexpected results**

Memory Collection

- **Tools for a full memory dump**
  - **AccessData FTK Imager Lite**
  - **Mandiant Memoryze**
  - **Monsools Windows Memory Toolkit**
  - **Belkasoft RAM Capturer**

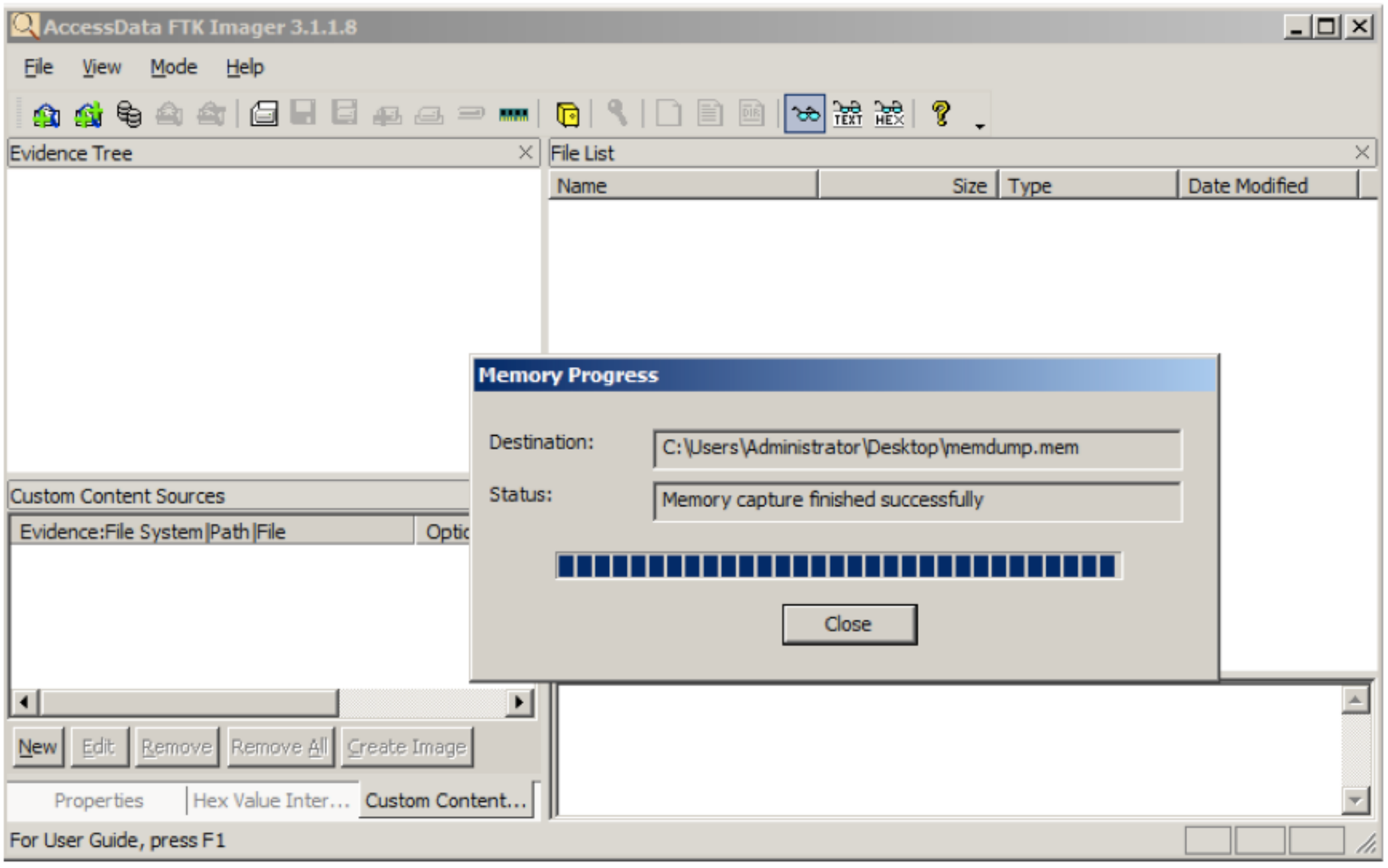
Mandiant Memoryze

- **Command-line tool: MemoryDD.bat**

```
<snip>
Beginning local audit.
Audit started 05-08-2012 20:21:23
Checking if 'D:\Downloads\LR\Memoryze\Audits\JASON-PC\2012050900
2123' exists...
Saving batch result to 'D:\Downloads\LR\Memoryze\Audits\JASON-PC
\20120509002123\'.
Batch results written to
'D:\Downloads\LR\Memoryze\Audits\JASON-PC\20120509002123\'.
Auditing (w32memory-acquisition) started 05-08-2012 20:21:23
Executing command for internal module w32memory-acquisition, 1.3.22.2
<Issue number="0" level="Info" summary="System range 0x0000000000000000 -
0x000000000009d000" context="EnumerateDevices"/>

<Issue number="7022" level="Warning" summary=
"Unable to read memory page(s)Invalid address range 0x00000000bf780000 -
0x00000000fffff000" context="MapPhysicalMemory"/>
```

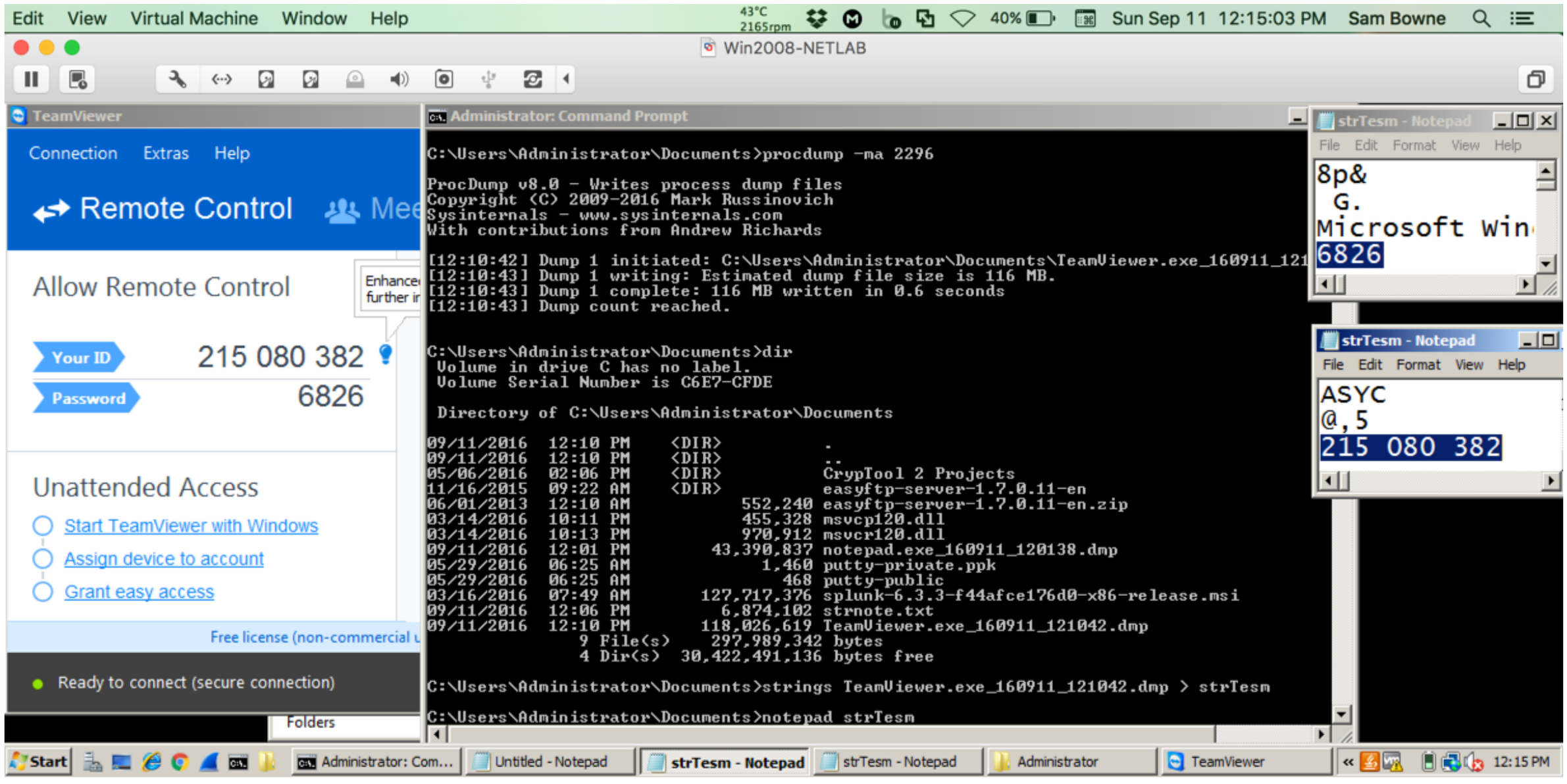
AccessData FTK Imager Lite



Individual Process RAM Dump

- **Tools**
  - **Mandiant Memoryze**
  - **Microsoft userdump**
  - **Microsoft procdump**
  - **Ntsecurity.nu pmdump**

TeamViewer Credentials



Live Data Collection on Unix-Based Systems

LINReS

- **From Network Intelligence India**
- **Written for RedHat 3 and 4, not updated since 2006**
- **Useful mainly as an example to guide you in making a custom tool**

Do It Yourself

- **Really the only option**
- **Make some scripts**
- **Mandiant uses Bourne shell scripts that make scripts for various Unix/Linux versions**
- **Requires constant maintenance**

Language Choices

- **Perl**
- **Python**
- **Bourne shell**
- **BASH (Mandiant uses this)**
- **others**

Apple Systems

- **system_profiler**
  - **Very long list of software, hardware, logs, etc.**

```
Applications:

    Microsoft Word:

      Version: 15.20
      Obtained from: Identified Developer
      Last Modified: 3/19/16, 9:38 AM
      Kind: Intel
      64-Bit (Intel): No
      Signed by: Developer ID Application: Microsoft Corporation (UBF8T346G9), Developer ID Certification Authorit$
      Location: /Applications/Microsoft Word.app
      Get Info String: 15.20 (160315), © 2016 Microsoft Corporation. All rights reserved.
```

system_profiler

```
    Media Player – Windows XP Professional:

      Version: VMware Fusion 8.0.2
      Obtained from: Identified Developer
      Last Modified: 3/22/16, 7:55 PM
      Kind: Intel
      64-Bit (Intel): Yes
      Signed by: Developer ID Application: VMware, Inc. (Fusion) (8J7TAMPT4P), Developer ID Certification Authorit$
      Location: /Users/sambowne/Downloads/CCTF/Win2/XP_Machine/Applications/Media Player – Windows XP Professional$
      Get Info String: Windows XP Professional
c:/windows/system32/mplay32.exe
```

```
Camera:

    FaceTime HD Camera:

      Model ID: Apple Camera VendorID_0x106B ProductID_0x1570
      Unique ID: DJH54345LFCG1HPBA
```

system_profiler

```
system.log:

  Description: System Log
  Date Modified: 9/14/16, 11:45 AM
  Size: 579 KB
  Contents: ...
```

```
Sep 14 11:12:55 Sams-MacBook-Pro-3 sharingd[278]: 11:12:55.688 : Purged contact hashes
Sep 14 11:12:55 Sams-MacBook-Pro-3 sharingd[278]: 11:12:55.689 : Discoverable mode changed to Off
Sep 14 11:12:55 Sams-MacBook-Pro-3 sharingd[278]: 11:12:55.689 : BTLE scanning stopped
Sep 14 11:12:55 Sams-MacBook-Pro-3 vmnet-bridge[79185]: Dynamic store changed
```

Built-in Unix Tools

Data Collected	Tool Name	License
System date and time	The date command	Part of operating system
Installed software	Debian-based: The dpkg --get-selections command RPM-based: The rpm -qa command BSD-based: The pkg_info command OS X: Copy the file /Library/Receipts/InstallHistory.plist	
File system information	The mount, df, and fdisk –l commands	Part of operating system
OS version	The cat /etc/issue command (Varies with operating system)	Part of operating system
Kernel version	The uname -a command	Part of operating system
Uptime	The w command	Part of operating system
Cron	Create a tar of cron files, normally kept in /var/spool/cron	Part of operating system

Built-in Unix Tools

Data Collected	Tool Name	License
Services	Varies by init system	Part of operating system
User accounts	The cat /etc/password and cat /etc/shadow commands	Part of operating system
Groups	The cat /etc/group command	Part of operating system
Network interfaces	The ifconfig -a command	Part of operating system
Routing table	The netstat -rn command	Part of operating system
ARP table	The arp -a command	Part of operating system
Network connections	The netstat -anp command	Part of operating system
Loaded drivers	Linux: The lsmod command BSD: The kldstat command OS X: The kextstat command (Varies for other operating systems)	Part of operating system

Built-in Unix Tools

Open files and handles	The lsof command	Free, commonly installed
Running processes and threads	Linux: The ps auxwwwem command (Varies for other operating systems)	Part of operating system
Configuration data (copy of files)	Create a tar of /etc (for example, tar cvfz /path/to/media/host-etc.tar.gz /etc/)	Part of operating system
System logs (copy of files)	Normally in /var/log or /var/adm or /Private/var/log (OS X), but varies between operating systems	Part of operating system
User shell history (copy of files)	BASH: .bash_history SH: .history (Varies with shell)	Part of operating system
File system listing	The find / -xdev –printf "%m;%Ax; %AT;%Tx;%TT;%Cx;%CT;%U;%G;% s;%p\n" command, or if find is not installed: The ls -alRu / command (atime) The ls -alRc / command (ctime) The ls -alR / command (mtime)	Part of operating system
LR output checksum computation	The md5 or md5sum command	Normally part of operating system

Memory Collection

- **The memory device is handled differently in every version of Unix, BSD, and Linux**
- **In earlier versions, you could just use dd to collect RAM through the /dev/mem device**
- **Direct access to memory is now blocked for security reasons**
- **Use LiME – Linux Memory Extractor (link Ch 7c)**

Loadable Kernel Modules

- **LiME is an LKM**
- **Must be compiled for the exact kernel version running on the target system**
- **No ability to include checksums of the output**
  - **You must do that yourself**

Collection from BSD-Based Kernels

- **Use dc3dd or dcfldd to capture contents of /dev/mem**
- **They are like dd but also include checksums**
- **In recent versions, there's no End Of File mark in /dev/mem, so you must manually specify how many bytes to capture**

Collection from Apple OS X

- **Memoryze for Mac (link Ch 7d)**
  - **Mac Memory Reader seems to be gone**

```
system1:memoryze4mac root# ./macmemoryze dump -f system1_memory.dd
INFO: loading driver...
INFO: opening /dev/mem...

INFO: dumping memory to [system1_memory.dd]
INFO: dumping 5637144576-bytes [5376-MB]
INFO: dumping [5637144576-bytes:5376-MB                              100%
INFO: dumping complete
INFO: unloading driver...
system1:memoryze4mac root#
```

Individual Process Dump

- **"gcore" (part of gdb, the GNU debugger)**

```
gcore -o /mnt/usb/case12-tag001-pid4327-sysauthd.img 4327
```

Ch 7b